BSI Seminar

Taj Hotel, Mumbai
15th April, 2008

Eight observations in support of this standard

The following is a summary of Dr. Brewer's address.

1. **Internal control**: Internal control is the means by which management marshals its resources to meet its objectives. There are two parts – (1) the processes for doing the job and (2) the processes for doing the job the way the boss wants it done. Every organisation has such a system, whether it is just doing what the boss tells you to do or a formal structure commonly found in larger organisations (particularly listed companies) it is still a system of internal control.

2. **Need for PDCA engine**: As identified in the UK Audit Practices Board guidance, explaining what financial directors should expect of external auditors in the wake of the first Turnbull report on corporate governance, you need a means to *establish*, *police* and *improve* your system of internal control. That engine is naturally predicated on the Deming PDCA cycle.

3. **Management systems are projections**: A management system as defined by a management system standard is merely a projection of some discipline, such as quality or environmental protection, onto your system of internal control. Thus all management systems are just subsets of internal control and should therefore be treated as such, i.e. they are all line management responsibilities that are owned by the Board of Directors.

4. **Time model**: The Brewer-List Time Model concerns measuring the effectiveness of your system of internal control. The model is expressed in terms of *events* and *impacts* where an impact has special significance: it is a happening that has a direct effect on the value of an organisation or on the quality of life. The model is based on the generally accepted accountancy principle of detecting the event in sufficient time to prevent the occurrence of an impact, but it has to deal with the case that your *preventive/detective* controls fail and you therefore need to react and recover from that impact. The model expresses these *reactive* controls in terms of various classes of Business Continuity Plans (BCPs). This clearly has something to do with BS 25999 and indeed BS 25999 provides a specification for those BCPs. There is however a greater significance I will return to later.

5. **Integrated management systems**: The existence of an integrated management system is implied by my third observation. Indeed BSI instructed the Committee that drafted BS 7799-2:2002 (now ISO/IEC 27001) to ensure that such integration would be possible. In practice it *is* possible. Gamma has such a system. I enjoy a single audit covering two standards. I have built

others elsewhere in the world. I build them in accordance with a robust theoretical model that has three components.

- First there is a Common PDCA framework. This comprises all the processes that I need to construct the PDCA engine that I have previously referred to. You need this to establish, police and improve your system of internal control, regardless of whatever business objectives you may have.

- The second is an AIL – an Alternative Ideas List. Its purpose is to act as a safety net in case your risk assessment/risk treatment process fails to identify an applicable control. Examples of AILs are Section 7 of ISO 9001, Annex A to ISO/IEC 27001 and CobiT. Quite often they are drawn from codes of best practice. AIL, by the way, is the French word for garlic. Where I come from garlic is used to ward off evil spirits, which in this context are the things that come back to haunt you when you have made a bad decision.

- The third is a specification for an essential process. The BS 25999 requirements for incident management and business continuity plans are excellent examples of this component.

6. **Technology exists but is not enough**: I have some technology to assist you to create an IMS. It is called IMS-Smart. It is hypertext driven, so literally your IMS documents and records are just one click away. The technology facilitates upgrades, so when a standard is revised updating the IMS documentation is simplified. It is currently being shipped with an ISO/IEC 27001, ISO 9001 and BS 25999 capability. It is a great product. However, technology, even technology as good as *IMS-Smart* is not enough.

7. **A management system is a management capability**: This is because a management system is first and foremost a management *capability*, albeit supported by documentation and records in conformity with some standard. Thus all implementation approaches must possess a high degree of technical transfer to create and sustain that management capability. This is true regardless of whether you employ an external consultant or source your implementation team exclusively in-house. Moreover, conformity is not demonstrated by documents that say what you *will* do. Admittedly there are documentation requirements and those documents must clearly exist. However, in the main, conformance is demonstrated through records of performance[1]. In other words, through evidence of what management *is doing now* and *has done in the past*.

8. **Every organisation has a requirement for a BCMS**: In conclusion let us return to my fourth observation. BS 25999 deals with the situation where the impact has occurred and it cares nothing about the triggering event. In other words that triggering event can be anything. All other management system standards, without loss of generality, aim to prevent the occurrence of the impact and say very little about recovery. ISO/IEC 27002 is a good case in

[1] There is an example of this our IMS demonstration. Open the demonstrator and follow the instructions. The first is a demonstration of conformance using this approach.

question. As a co-author of that standard I am actually embarrassed about what is says about business continuity, which in my view has always been inadequate. Moreover each of these other management system standards deals only with particular triggering events. For example, my research has shown that ISO/IEC 27001 and ISO 9001 each deal with three. I have given them names in attempt to describe what they are. The triggering events for ISO/IEC 27001 are *vulnerability exploitation*, *IT failure* and *dispossession* (of a container of information). Together these three events map to all 133 controls in Annex A to that standard. The triggering events for ISO 9001 are *introduction of nonconformity* (into your product), *wrong product* (i.e. your product meets its specification but it wasn't what the customer wanted) and *dissatisfied customer* (e.g. despite the fact that you sold the customer the correct product and it meets its specification to perfection, your customer is dissatisfied with the way you dealt with him/her.) Clearly, these triggering events are quite distinct. Those for other management system standards are as just as distinct as well. You may be correct to assume, for example, that a particular triggering event for ISO 14001 concerns *contamination*. BS 25999 must deal with all of these triggering events *plus one*, and that event is quite simply the one that nobody thought of (and 9/11 may be a good example of that). Thus BS 25999 deals with the triggering events of all other management system standard plus one. It deals with reaction/recovery to the occurrence of impacts whereas other management system standards primarily address prevention of impact. Not every organisation needs ISO 9001 and ISO 14001 and ISO/IEC 20000-1 and ISO 22000 and ISO/IEC 27001, etc., but you all need BS 25999. There are over ½ million ISO 9001 registrations. There will be significantly more BS 25999 registrations. BS 25999 is an essential component of internal control. You must have one. Why not build yours now?